U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability

Development and Demonstration of a Security Core Component

Near-real-time cyber and physical security situational awareness capability for the control system environment

Background

Control systems used in energy infrastructure are susceptible to cybersecurity related threats and even the best cyber defenses may fail when up against a committed adversary.

Energy management systems (EMS) are used in the electric grid to monitor, control and optimize the generation, transmission and distribution networks of the grid. While EMS operators are trained in managing these systems, they are generally not trained in managing the security of computer networks. Furthermore, existing EMS tools do not assist operators in doing so.

Barriers

- Visualizing the security posture of a wide range of disparate data of varying granularity is difficult
- Supervisory control and data acquisition (SCADA) and EMS systems are complex and widely distributed
- Energy control center EMS operators often lack the training, expertise and tools needed to manage computer networks

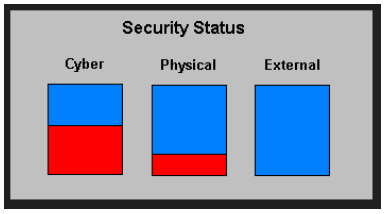
Project Description

This project will produce a software solution that provides operators with the tools and training to respond effectively and assertively to cyber threats. The project team will develop and demonstrate a centralized software component, the Cyber Security Manager (CSM), for SCADA, EMS and distribution management systems (DMS). CSM will monitor the wide variety of security-related components of EMS systems and provide a centralized cybersecurity situational awareness and control capability for EMS operators.

The concepts and operation of CSM will be simulated and incorporated into Siemens' existing Operator Training Simulator (OTS). The software will be demonstrated on both the factory and live system scales.

Siemens will use its EMS and OTS software as well as prototype software previously developed by Pacific Northwest National Laboratory as central components for the development of this technology.

Prototype display of the "Status Widget"



Benefits

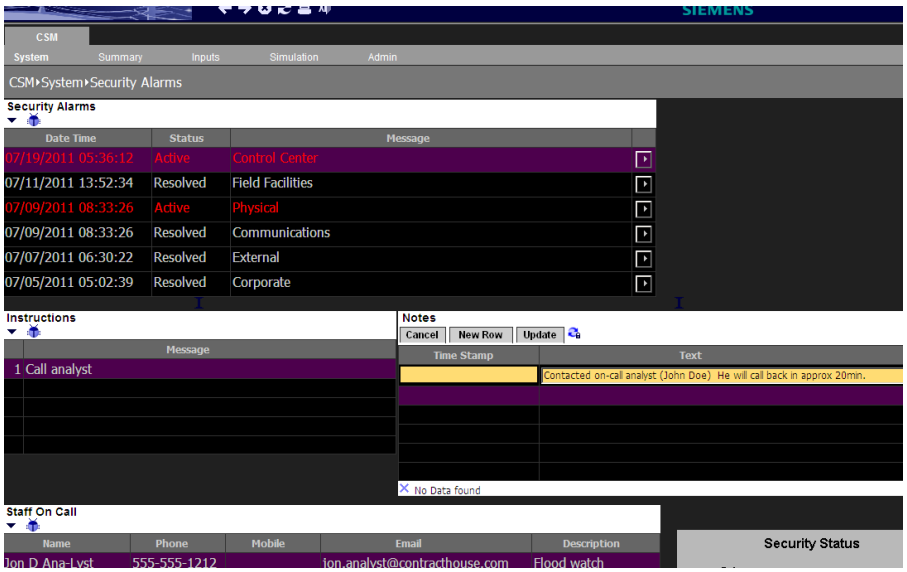
- Accepts, analyzes and correlates data from security components of Supervisory Control and Data Acquisition (SCADA), EMS and DMS systems and supporting network infrastructure
- Enables operators to detect signs of an attack on the system and its infrastructure
- Produces a view of the cybersecurity status of the SCADA or EMS system and its infrastructure
- Provides a set of workflow-based guidance to aid decision making
- Permits operators to receive life-like training in the use of CSM and develop and practice defense procedures
- Generates technology that is customizable and transferable to other energy infrastructures

Partners

- Siemens Energy, Inc.
- Pacific Northwest National Laboratory
- Sacramento Municipal Utilities District
- Omaha Public Power District
- CenterPoint Energy
- New York Power Authority
- Westar Energy

Control Room

CSM Display Prototype of an operator adding a note to a "Control Center" alarm



Technical Objectives

The project consists of research, development and demonstration efforts that will produce an integrated cybersecurity monitoring system for energy control centers.

Phase 1: Research and Development

- Develop and review requirement specifications
- Design and review the CSM core, and develop and test the CSM core engine
- Interface the intrusion detection system (IDS) and log management system to CSM
- Enhance OTS to include CSM features
- Add the SCADA "points" required by CSM
- Interface the Bandolier scanning results to CSM
- Develop a network traffic capture utility
- Perform enhancements to permit the CSM status widget to be added to existing displays
- Develop CSM user interface, documentation, and training

Phase 2: Demonstration

- Install the software onto a field support system at Siemens and perform factory acceptance testing
- Conduct administrator and user training
- Install the software onto a live system and perform site acceptance testing

End Results

Project results will include:

- A cybersecurity monitoring system for energy control centers that is integrated into an environment that is familiar to operators
- A vehicle for training operators of any electric utility and allowing control centers to simulate scenarios and test responses in order to develop effective response methodologies and practices
- Technology that has been successfully demonstrated, is commercially viable, and is transportable to other energy infrastructures

August 2012

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE) R&D Program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyber attacks.

For More Information:

Carol Hawk
Program Manager
DOE OE R&D
202-586-3247
carol.hawk@hq.doe.gov

Dave Taylor, CISSP
Cyber Security Consultant
Siemens Energy, Inc.
952-607-2140
dtaylor@siemens.com

Visit Our Website:

http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity